**UNITED STATES DISTRICT COURT**
**MIDDLE DISTRICT OF TENNESSEE**
**NORTHEASTERN DIVISION**

| | |
|---|---|
| TROY COLLINS, on behalf of himself and all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>CASH EXPRESS, LLC,<br><br>Defendant. | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiff Troy Collins ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Cash Express, LLC ("Cash Express" or "Defendant"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

## I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information that consumers entrusted to it, including, without limitation their names, dates of birth, contact information, government identification (such as Social Security numbers and driver's license numbers, medical details, and financial information such as bank account and routing numbers.[1]

2. Cash Express is a loan company, dealing with "payday" loans, installment loans, small lines of credit, gold purchases, title loans, and check cashing services.

3. On or around February 6, 2022, Defendant determined that unauthorized, unknown

[1] Exhibit 1 (*Website Notice* posted on the Cash Express website).

third parties had gained access to Defendant's internal computer system between January 29, 2022 and February 6, 2022 (the "Data Breach").

4. During the Data Breach, the attacker had access to the personally identifiable information[2] and protected health information ("PHI") (collectively, "Personal Information") of more than 106,000 consumers, including Plaintiff, who used Defendant's services.

5. Although Defendant learned of the Data Breach in February 2022, Defendant did not begin notifying Plaintiff and Class Members until at least August of 2022.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Personal Information, Defendant assumed legal and equitable duties to those individuals.

7. The accessed Personal Information of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted Personal Information to criminals. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. Indeed, Defendant has already cautioned Plaintiff and Class Members to "remain vigilant for unauthorized financial activity" and has directed them to take a variety of affirmative steps to protect themselves from further harm.[3]

9. This Personal Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Personal Information of Plaintiff and

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[3] *See* Exhibit 1.

Class Members.

10. Plaintiff brings this action on behalf of all persons whose Personal Information was compromised as a result of Defendant's failure to: (i) adequately protect the Personal Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the Personal Information of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of their Personal Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their Personal Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information; (c) likely remains freely available for cybercriminals to use and abuse on the Dark Web.

12. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Personal Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption

of data, even for internal use. As the result, the Personal Information of Plaintiff and Class Members was compromised through disclosure to and exfiltration by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## II. PARTIES

13. Plaintiff Troy Collins is a citizen of Tennessee residing in Monroe County, Tennessee. Plaintiff has a loan procured through Cash Express and was, at all relevant times, a consumer of Cash Express services.

14. On or about September 15, 2022, Plaintiff received a Notice of Data Breach in the mail from Defendant stating that his Personal Information had been compromised.

15. Defendant Cash Express LLC. is a Tennessee limited liability corporation headquartered at 345 S. Jefferson Avenue, Suite 403, Cookeville, Tennessee 38501.

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

17. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

## III. JURISDICTION AND VENUE

18. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d) ("CAFA"), as the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. Upon information and belief, there are more than 100 Class Members, a number of whom are citizens of states different from that of the Defendant.

19. This Court has personal jurisdiction over Defendant because Cash Express is headquartered in Tennessee, regularly conducts business in this District, and maintains its principal place of business in this District.

20. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391(b)(2) because the Defendant's principal places of business is in this District and a substantial part of the events or omissions giving rise to this action, particularly decisions related to data security and the acts which lead to the Data Breach, occurred in this District.

## IV. FACTUAL ALLEGATIONS

***Background***

21. Cash Express is a loan company, dealing in "payday" loans, installment loans and small lines of credit, gold purchases, title loans and check cashing services.

22. In the normal course of business, for the services that Cash Express provides, Cash Express collects and stores some of Plaintiff's and Class Members' most sensitive and confidential information, including their Social Security numbers. Cash Express collects this Personal Information from consumers, like Plaintiff and Class Members, who complete forms and applications, both online and in a Cash Express location to obtain various types of loans.

23. On its website, Cash Express has a posted Privacy Policy that states, in part:

> Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do
>
> The types of personal information we collect and share depend on the product or service you have with us. This information can include:
> - Social Security number and income
> - transaction history and employment information
> - overdraft history and checking account information

> All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Cash Express chooses to share; and whether you can limit this sharing.[4]

24. The Privacy Policy explains that Cash Express can share Personal Information for business purposes, such as to process transactions, maintain accounts, or respond to court order and legal investigations. It also explains that Cash Express can share Personal Information for its own marketing purposes and marketing with other financial companies. The circumstances of the Data Breach did not constitute Cash Express sharing Personal Information for business or marketing purposes.

25. Plaintiff and Class Members relied on this sophisticated Defendant's promises to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their Personal Information.

26. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Personal Information from involuntary disclosure to third parties.

27. This case involves a breach of a computer system that resulted in the unauthorized access, disclosure, and/or acquisition of the Personal Information of Plaintiff and Class Members to unknown third-parties. As a result of Defendant's failure to implement and follow basic security procedures, the Personal Information of Plaintiff and Class Members was more likely than not accessed, disclosed, and/or acquired and is now in the hands of criminals.

28. Once information is placed onto the internet, it is virtually impossible to remove.

[4] *See* https://www.cashexpressllc.com/uploads//Cash_Express_Privacy_Policy_July_2021.pdf (last accessed Oct. 16, 2022).

Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Defendant's failures.

29. Additionally, as a result of Defendant's failure to follow industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services Defendant was to provide.

30. By obtaining, collecting, using, and deriving a benefit from the Personal Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access, intrusion, and/or acquisition.

31. Moreover, Defendant now puts the burden squarely on Plaintiff and Class Members to take steps to protect themselves. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[5]

32. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[6] leisure time is defined as time not occupied with work or chores and is "the time equivalent

[5] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, *available at* https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last visited Aug. 2, 2022); *see also* U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data, available at* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last visited Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[6] *See* https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (last visited Aug. 2, 2022).

of 'disposable income.'"[7] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

33. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

***The Data Breach***

34. On or about February 6, 2022, Cash Express became aware of unusual activity on its network. It was subsequently determined that an unauthorized third-party gained access to the Cash Express computer system which resulted in the unauthorized access to the sensitive Personal Information belonging to Plaintiffs and Members of the Class.

35. Cash Express determined the third party had access to Personal Information from January 29, 2022 and February 6, 2022. The sensitive Personal Information included: names, dates of birth, contact information, government identification (Social Security numbers and driver's license numbers), medical details, and financial information such as bank account and routing numbers.

36. Cash Express claims to have hired third-party experts to address the Data Breach, perform an investigation into the unauthorized activity, and further secure its systems to protect customer information.

37. Despite learning of the Data Breach in February 2022, Defendant did not begin

[7] *Id.*

notifying Plaintiff and Class Members until approximately September 2022, nearly seven months after the Data Breach first occurred.

38. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have still not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

39. The occurrence of the Data Breach indicates that Defendant failed to adequately implement industry-standard measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Personal Information of more than 106,000 individuals, including Plaintiff and Class Members.

***Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Personal Information.***

40. In the course of its regular business operations, Defendant acquired, collected, and stored Plaintiff's and Class Members' Personal Information.

41. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly confidential Personal Information.

42. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Personal Information from disclosure.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Personal Information and relied on Defendant to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***Securing PII and Preventing Breaches***

44. Defendant could have prevented this Data Breach by properly securing and encrypting the Personal Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially that of former customers.

45. Defendant's negligence in safeguarding the Personal Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

46. Indeed, on its website, Defendant provides resources for customers regarding tips on how to safeguard Personal Information from theft. In the source Defendant shares with its customers, customers are warned: "When your personal financial information gets in the wrong hands, the consequences can be devastating. It's critical to understand how identity theft and card fraud can happen to you."[8]

47. The source further provides: "Be careful with your Social Security Number[.] Your social security number is a major target for identity thieves because it can give them access to your credit report and bank accounts."[9] Here, Defendant's actions resulted in the exposure of not only Plaintiff's and Class Member's Social Security numbers, but also their bank account and financial information, a devastating combination.

48. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Personal Information of Plaintiff and Class Members from being compromised.

49. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

[8] *See* https://www.cashexpressllc.com/uploads/drs_9.pdf (last accessed Oct. 19, 2022).
[9] See i*d.*

committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

50. The ramifications of Defendant's failure to keep secure the Personal Information of Plaintiff and Class Members are long lasting and severe. Once stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

***Value of Personal Identifiable Information***

51. The Personal Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[14]

52. Social Security numbers, for example, are among the worst kind of personal

[10] 17 C.F.R. § 248.201 (2013).
[11] *Id*.
[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 4, 2022).
[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 4, 2022).
[14] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 4, 2022).

information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[15]

53. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

54. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

[15] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 2, 2022).
[16] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 1, 2022).

breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and date of birth.

56. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[17]

57. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

58. The Personal Information of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the Personal Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

59. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

---

[17] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 1, 2022).

[18] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last visited Oct. 2, 2022).

60. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Personal Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

61. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

62. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

63. Further, there is a market for Plaintiff's and Class Members PHI, and the stolen PII has inherent value.

64. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

65. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed

with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

66. Defendant still has not shared with Plaintiff or Class Members what "limited medical information" was involved in the Data Breach.

67. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Personal Information of Plaintiff and Class Members.

***Plaintiff's Experience***

68. Plaintiff has a loan procured through Cash Express and is a Cash Express consumer.

69. As a condition of receiving a loan from Cash Express, Plaintiff provided Cash Express with his name, address, telephone number, date of birth, Social Security number, and other Personal Information.

70. Upon information and belief, Plaintiff's Personal Information was in Defendant's computer systems during the Data Breach and remains in Defendant's possession.

71. Plaintiff received a Notice of Data Breach from Defendant on or about September 15, 2022. The letter stated that Plaintiff's Personal Information was compromised in the Data Breach.

72. As a result of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through

[19] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), *available at* https://khn.org/news/rise-of-indentity-theft/ (last visited Aug. 2, 2022).

his unsolicited emails and text messages, time spent verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

73. As a result of the Data Breach, Plaintiff has suffered from actual misuse of his Personal Information. After the Data Breach, Plaintiff experienced unauthorized charges on his Social Security card, resulting in the loss of Plaintiffs' monthly money. Plaintiff was initially unable to pay his bills due to lack of funds and spent several hours on the phone with Social Security Administration and conducting research trying to resolve the issues. To date, the issues are still not resolved as Plaintiff has not been fully reimbursed.

74. Plaintiff is very careful about sharing his Personal Information. He has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source.

75. Plaintiff stores any documents containing his Personal Information in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

76. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Personal Information—a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving services from Defendant, which was compromised in and as a result of the Data Breach.

77. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

78. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his Personal Information, especially his Social Security number, in

combination with his name, being placed in the hands of unauthorized third parties and criminals. This injury was worsened by Defendant's continuing delay in revealing the true nature of the threat to Plaintiff's Personal Information.

79. Plaintiff has a continuing interest in ensuring that his Personal Information, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

## V. CLASS ALLEGATIONS

80. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

81. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose Personal Information was compromised during the Data Breach referenced in the Website Notice published by Defendant on or around September 12, 2022 (the "Nationwide Class"

82. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

83. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

84. This action is brought and may be maintained as a class action because there is a

well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant classwide relief because Plaintiff and all members of the Nationwide Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

85. The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least 106,000 Class Members.

86. Common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the Personal Information of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the Personal Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Personal Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Personal Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Personal Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Personal Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Personal Information of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

87. Plaintiff is a member of the Classes he seeks to represent and his claims and injuries are typical of the claims and injuries of the other Class Members.

88. Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiff and his counsel.

89. Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

90. A class action is superior to other available means for fair and efficient adjudication

of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

## COUNT I
**Negligence**
**(On Behalf of Plaintiff and the Nationwide Class)**

91. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 79.

92. Plaintiff and the Nationwide Class provided and entrusted Defendant with certain Personal Information as a condition of receiving medical services and care based upon the premise and with the understanding that Defendant would safeguard their information, use their Personal Information for business purposes only, and/or not disclose their Personal Information to unauthorized third parties.

93. Defendant has full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the Personal Information were wrongfully disclosed.

94. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Personal Information of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

95. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Personal Information of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

96. Defendant owed a duty to Plaintiff and the Nationwide Class to implement intrusion detection processes that would detect a data breach or unauthorized access to its systems in a timely manner.

97. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Personal Information it was no longer required to retain pursuant to regulations, including that of former patients.

98. Defendant also had a duty to employ proper procedures to detect and prevent the improper access, misuse, acquisition, and/or dissemination of the Personal Information of Plaintiff and the Nationwide Class.

99. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential Personal Information, a necessary part of their relationships with Defendant.

100. Defendant owed a duty to disclose the material fact that Defendant's data security

practices were inadequate to safeguard the personal and medical information of Plaintiff and the Nationwide Class.

101. Defendant's Privacy Policies acknowledge Defendant's duty to adequately protect the personal and medical information of Plaintiff and the Nationwide Class.

102. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

103. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on Defendant's systems.

104. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Personal Information of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendant.

105. Plaintiff and the Nationwide Class had no ability to protect their Personal Information that was in, and likely remains in, Defendant's possession.

106. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

107. Defendant had and continues to have a duty to adequately disclose that the Personal

Information of Plaintiff and the Nationwide Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

108. Defendant has admitted that the Personal Information of Plaintiff and the Nationwide Class was wrongfully accessed, acquired, and/or released to unauthorized third persons as a result of the Data Breach.

109. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Personal Information of Plaintiff and the Nationwide Class during the time the Personal Information was within Defendant's possession or control.

110. Defendant improperly and inadequately safeguarded the Personal Information of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

111. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Personal Information of Plaintiff and the Nationwide Class in the face of increased risk of theft.

112. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect unauthorized access or intrusions and prevent dissemination of their Personal Information. Additionally, Defendant failed to disclose to Plaintiff and the Nationwide Class that Defendant's

security practices were inadequate to safeguard the Personal Information of Plaintiff and the Nationwide Class.

113. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Personal Information it was no longer required to retain pursuant to regulations, including PII of former patients and employees.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

115. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Personal Information of Plaintiff and the Nationwide Class would not have been compromised.

116. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Personal Information of Plaintiff and the Nationwide Class was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

117. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer injury.

118. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

119. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

**COUNT II**
**Negligence Per Se**
**(On Behalf of Plaintiff and the Nationwide Class)**

120. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 79.

121. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

122. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

123. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

124. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

125. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

126. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Personal Information is used; iii) the compromise, publication, and/or theft of their Personal Information ; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information ; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Personal Information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

## COUNT III
## Breach of Implied Contract
## (On Behalf of Plaintiff and the Nationwide Class)

127. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 79.

128. Defendant required Plaintiff and the Nationwide Class to provide and entrust their Personal Information as a condition of obtaining services from Defendant.

129. Plaintiff and the Nationwide Class paid money to Defendant in exchange for goods and services, as well as Defendant's promises to protect their Personal Information from unauthorized disclosure.

130. As a condition of obtaining services from Defendant, Plaintiff and the Nationwide Class provided and entrusted their Personal Information. In so doing, Plaintiff the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

131. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete Personal Information and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Personal Information.

132. Plaintiff and the Nationwide Class Members would not have entrusted their Personal Information to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential Personal Information.

133. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

134. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by making their Personal Information accessible (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the Personal Information was secure, failing to encrypt Plaintiff and Class Members' sensitive Personal Information, failing to safeguard and protect their

Personal Information, and by failing to provide timely and accurate notice to them that Personal Information was compromised as a result of the data breach.

135. Defendant's failures to meet these promises constitute breaches of the implied contracts.

136. Because Defendant allowed unauthorized access to Plaintiff and Class Members' Personal Information and failed to safeguard the Personal Information, Defendant breached its contracts with Plaintiff and Class Members.

137. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiff and Class Members that were of a diminished value.

138. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the diminished value of services provided by Defendant; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

139. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class, and appointing Plaintiff and his Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the

Personal Information of Plaintiff and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a

breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, nominal, and statutory

damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff, by counsel, hereby demands that this matter be tried before a jury.

Date: October 27, 2022

By:

/s/ Christopher N. Coyne
CHRISTOPHER N. COYNE, TNBPR#032047
**MORGAN & MORGAN-NASHVILLE, PLLC**
810 Broadway, Suite 105
Nashville, TN 37203
(615) 780-6322
ccoyne@forthepeople.com

JEAN S. MARTIN
(*Pro Hac Vice application forthcoming*)
FRANCESCA KESTER
(*Pro Hac Vice application forthcoming*)
**MORGAN & MORGAN COMPLEX LITIGATION GROUP**
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

*Attorneys for Plaintiff and the Putative Class*